GEOMETRIC STRUCTURE OF SUMSETS

JAEWOO LEE

Abstract. Given a finite set of lattice points, we compare its sumsets and lattice points in its dilated convex hulls. Both of these are known to grow as polynomials. Generally, the former are subsets of the latter. In this paper, we will see that sumsets occupy all the central lattice points in convex hulls, giving us a kind of approximation to lattice points in polytopes.

1. Introduction

Let A be a a set of lattice points in dimension n. For any nonnegative integer h, we define the *h-fold sumset* $hA = \{a_1 + a_2 + \ldots + a_h : a_1, a_2, \ldots, a_h \in A\}$. And the *dilation* is $h * A = \{ha : a \in A\}$.

A *hyperplane* H is the set $\{x \in \mathbb{R}^n : (x, u) = \alpha\}$ for some nonzero $u \in \mathbb{R}^n$ and some number α, where $(\cdot\,,\cdot)$ indicates an inner product in $\mathbb{R}^n$. The vector u is called a *normal vector* to H. A hyperplane divides $\mathbb{R}^n$ into two closed half-spaces H^+ and H^- where

$$H^+ = \{x \in \mathbb{R}^n : (x, u) \geq \alpha\}$$
$$H^- = \{x \in \mathbb{R}^n : (x, u) \leq \alpha\}\,.$$

We write $d(x, y)$ to denote the distance between two points $x, y \in \mathbb{R}^n$. If $S, T \subseteq \mathbb{R}^n$, then

$$d(x, S) = \inf_{s\in S} d(x, s)\,,$$
$$d(S, T) = \inf_{s\in S, t\in T} d(s, t)\,.$$

In particular, the distance from a point $x \in \mathbb{R}^n$ to a hyperplane H where $x \notin H$, is given by the length of the perpendicular line segment from x to H.

If two hyperplanes H_1, H_2 are parallel, their normal vectors are multiples of each other, so we can take a single normal vector u and write $H_1 = \{x : (x, u) = \alpha_1\}$ and $H_2 = \{x : (x, u) = \alpha_2\}$. Take any $x \in H_1$. Then $d(x, H_2)$ is given by the perpendicular line segment. To calculate

Date: April 25, 2007.

2000 *Mathematics Subject Classification.* Primary: 11H06, 11P21; Secondary: 52B20.

Key words and phrases. sumset, polytope, lattice points.

the distance between H_1 and H_2, note that $x + tu$ where $t \in \mathbb{R}$ gives the perpendicular ray from x to H_2 . If the ray meets H_2 when $t = t_2$, then $t_2 = (\alpha_2 - \alpha_1)/|u|^2$. Thus, $d(x, H_2) = |t_2 u| = (\alpha_2 - \alpha_1)/|u|$, which is independent of the choice of x. Therefore, when H_1 and H_2 are parallel, $d(H_1, H_2)$ is given by the length of any perpendicular line segment joining them.

A *polytope* is the convex hull of a finite set of points in some $\mathbb{R}^n$, or equivalently, a bounded set which is an intersection of finitely many closed half-spaces. Let $\Delta = \mathrm{conv}(a_1, a_2, \ldots, a_m)$ where $a_i \in \mathbb{Z}^n$. Then define the *dilation of* Δ , $h * \Delta$, as

$$\begin{aligned} h * \Delta &= \{hx : x \in \Delta\} \\ &= \{\sum \lambda_i a_i : \lambda_i \geq 0, \sum \lambda_i = h\} \\ &= \mathrm{conv}(ha_1, \ldots, ha_m) . \end{aligned}$$

Assume that $\Delta \subseteq \mathbb{R}^n$ is an n-dimensional nonempty lattice polytope, and h is a positive integer. Then Ehrhart [1] showed that there is a polynomial $p(h)$, called the *Ehrhart polynomial*, such that

$$|(h * \Delta) \cap \mathbb{Z}^n| = p(h)$$

where

$$p(h) = \mathrm{Vol}(\Delta)h^n + \frac{\mathrm{Vol}(\partial(\Delta))}{2} h^{n-1} + \cdots + \chi(\Delta) .$$

Here, $\chi(\Delta)$ is the Euler characteristic of Δ, and $\mathrm{Vol}(\partial(\Delta))$ is the surface area of Δ normalized with respect to the sublattice on each face of Δ.

If $\Delta = \mathrm{conv}(A)$ where A is a finite set of integral points in some $\mathbb{R}^n$, then $|(h * \Delta) \cap \mathbb{Z}^n| \geq |hA|$. Then we can consider the growth of $|hA|$ instead. Nathanson [6] proved that the growth of $|hA|$ is a linear function when A is a subset of integers normalized in a way. When $A_1, A_2, \ldots, A_r$ and B are finite subsets of $\mathbb{N}_0$, normalized similarly as above, then Han, Kirfel, and Nathanson [2] showed that $|B + h_1 A_1 + \cdots + h_r A_r|$ is a multilinear function of $h_1, \ldots, h_r$ eventually. Furthermore, if $A_1, A_2, \ldots, A_r$ and B are finite subsets of an abelian semigroup which contains 0, then $|B + h_1 A_1 + \cdots + h_r A_r|$ is a polynomial of $h_1, \ldots, h_r$ for all sufficiently large $h_1, \ldots, h_r$, which was proved by Khovanskiĭ [4] when $r = 1$, and by Nathanson [7] for $r \geq 2$. And if A, B are finite subsets of an abelian group without elements of finite order, then Khovanskiĭ [4] computed the degree and the leading coefficient of the polynomial above (actually his proof contained a gap, but the gap is fixed by the work of this paper).

In this paper, we will investigate the growth of the sumset hA from the geometric point of view.

2. Khovanskiĭ's Lemmas

Our paper starts with lemmas that Khovanskiĭ proved in [4]. Let A be a finite subset of $\mathbb{Z}^n$, $A = \{a_1, \dots, a_m\}$, with $|A| = m$ and $\Delta = \operatorname{conv}(A)$. Also assume that A generate $\mathbb{Z}^n$ as a group.

Lemma 1. *There exists a constant C with the following property: for all linear combination $\sum \lambda_i a_i$ of $a_i \in A$ with real coefficients λ_i such that $\sum \lambda_i a_i$ is an integral point, there exists a linear combination $\sum n_i a_i$ of a_i with integer coefficients n_i such that $\sum n_i a_i = \sum \lambda_i a_i$, with $\sum |n_i - \lambda_i| < C$.*

Proof. Let $X = \{x : x \in \mathbb{Z}^n, x = \sum \lambda_i a_i,\ \text{with } 0 \le \lambda_i \le 1\}$, which is a finite set. Since A generate $\mathbb{Z}^n$, each $x \in X$ can be written as $x = \sum_{i=1}^m n_i(x) a_i$, where $n_i(x) \in \mathbb{Z}$. So for each $x \in X$, we fix one representation $\sum_{i=1}^m n_i(x) a_i$ with $n_i(x) \in \mathbb{Z}$. Let $q = \max_{x \in X} \sum_{i=1}^m |n_i(x)|$ and let $C = m + q$, a positive integer. Then for any $z = \sum \lambda_i a_i \in \mathbb{Z}^n$, $x = z - \sum [\lambda_i] a_i \in X$. So $x = \sum_{i=1}^m n_i(x) a_i$ with $n_i(x) \in \mathbb{Z}$ and $z = \sum_{i=1}^m \big(n_i(x) + [\lambda_i]\big) a_i = \sum_{i=1}^m \lambda_i a_i$ with $\sum |n_i(x) + [\lambda_i] - \lambda_i| < \sum_{i=1}^m \big(|n_i(x)| + 1\big) \le q + m = C$. □

Let h be a positive integer and assume $0 \in A$. Then

$$\Delta = \{\sum \lambda_i a_i : \lambda_i \ge 0, \sum \lambda_i \le 1\}$$

and

$$h * \Delta = \{\sum \lambda_i a_i : \lambda_i \ge 0, \sum \lambda_i \le h\}.$$

Define

$$\Delta(h, C) = \{\sum \lambda_i a_i : \lambda_i \ge C, \sum \lambda_i \le h - C\}$$

with C as in Lemma 1.

Then, if $x = \sum \lambda_i a_i \in \Delta(h, C)$, let $\lambda_i = \alpha_i + C,\ \alpha_i \ge 0$. So

$$\begin{aligned}
\Delta(h, C) &= \{\sum (\alpha_i + C) a_i : \alpha_i \ge 0, \\
&\qquad \sum \alpha_i \le h - C - mC\} \\
&= C \sum a_i + \{\sum \alpha_i a_i : \alpha_i \ge 0, \\
&\qquad \sum \alpha_i \le h - C - mC\} \\
&= C \sum a_i + (h - C - mC) * \Delta.
\end{aligned}$$

Note $\Delta(h, C)$ is an empty set when $h < C + mC$, a single point $C \sum a_i$ when $h = C + mC$, and a dilation of Δ translated by an integral point when $h \ge C + mC + 1$.

Let $\mathbb{Z}^n(A)$ be the group generated by the differences of the elements of A.

Lemma 2. *Assume $\mathbb{Z}^n(A) = \mathbb{Z}^n$, and $0 \in A$. Then, every integral point in $\Delta(h, C)$ belongs to the sumset hA.*

Proof. Let z be an integral point in $\Delta(h, C)$. Then

$$z = \sum \lambda_i a_i, \quad \lambda_i \geq C\,, \sum \lambda_i \leq h - C\,.$$

By Lemma 1, $z = \sum n_i a_i$, $n_i \in \mathbb{Z}$, $\sum |n_i - \lambda_i| < C$. If $n_i < 0$ for some i, then $|n_i - \lambda_i| > C$. Therefore, all n_i must be nonnegative. And $\sum n_i = \sum |n_i| = \sum |n_i - \lambda_i + \lambda_i| \leq \sum |n_i - \lambda_i| + \sum |\lambda_i| < C + h - C = h$. Thus $z = \sum n_i a_i$, $n_i \geq 0$, $\sum n_i < h$. Since $0 \in A$,

$$hA = \{ \sum n_i a_i : n_i \geq 0, \sum n_i \leq h \}\,,$$

therefore $z \in hA$. □

Using these results, Khovanskiĭ in [4] gave an argument for the following theorem, but the argument contained an error about boundary points. For details and how to modify his arguments to get a similar result on simplex, see [5].

Theorem 3. *Suppose $\mathbb{Z}^n(A) = \mathbb{Z}^n$. Then, there exists a constant ρ with the following property: for any positive integer h, every integral point of $h * \Delta$, whose distance to $\partial(h * \Delta)$ is more than ρ, belongs to hA.*

The condition $\mathbb{Z}^n(A) = \mathbb{Z}^n$ implies that the dimension of Δ is n. In general, hA is a proper subset of $(h * \Delta) \cap \mathbb{Z}^n$. Theorem 3 states that hA takes all of the central region in $h * \Delta$.

3. Proof of Theorem

Now we prove Theorem 3.

PROOF OF THEOREM 3. Take any hyperplane

$$H = \{x : (x, u) = \alpha\}.$$

Then, for a positive integer h,

$$h * H = \{x : (x, u) = h\alpha\},$$

so the dilation of a hyperplane results in another hyperplane which is parallel to the original one. And

$$H - b = \{x : (x, u) = \alpha - (b, u)\}$$

where $b \in \mathbb{R}^n$, so the translation of a hyperplane is a hyperplane that is parallel to the original one as well.

Now, let's calculate the distance between

$$H_1 = h * H\,,$$

$$H_2 = g * H - b,$$

where $h > g$, h, g are positive integers, and $b \in \mathbb{R}^n$. Then $H_1 = \{x : (x, u) = h\alpha\}$, $H_2 = \{x : (x, u) = g\alpha - (b, u)\}$, so H_1 is parallel to H_2. Take any point $x_1 \in H_1$. Then $x_1 + tu$, $t \in \mathbb{R}$ is a ray perpendicular to both H_1 and H_2. Let's say $x_1 + tu \in H_2$ when $t = t_2$. Then

$$t_2 = \frac{(g-h)\alpha - (b, u)}{|u|^2}\,,$$

$$d(H_1, H_2) = |t_2 u| = \frac{|(g-h)\alpha - (b, u)|}{|u|}\,.$$

Without loss of generality, we may assume $0 \in A$ because, if not, take any $a \in A$ which is also a vertex of Δ. Then take $\bar{\Delta} = \Delta - a$ so that $0 \in \bar{\Delta}$. Then $\bar{\Delta} = \text{conv}(A-a)$ and $h*\bar{\Delta} = h*\Delta - ha = h*\text{conv}(A-a)$. And, for any positive integer h, if $x \in (h*\Delta) \cap \mathbb{Z}^n$ with $d(x, \partial(h*\Delta)) > \rho$, then $x - ha \in h * \bar{\Delta}$, and $d(x - ha, \partial(h*\bar{\Delta})) > \rho$ since a translation doesn't change the distance. Thus $x - ha \in h(A-a) = hA - ha$. So $x \in hA$, proving our claim.

Let $h \geq C + mC + 1$. Recall

$$\Delta(h, C) = C \sum a_i + (h - C - mC) * \Delta.$$

Let $\Delta = G_1^+ \cap \ldots \cap G_l^+$ where G_i's are hyperplanes $\{x : (x, u_i) = \alpha_i\}$ with $G_i \cap \Delta \neq \emptyset$. Then $h * \Delta = H_1^+ \cap \ldots \cap H_l^+$ and $\Delta(h, C) = H_1^{'+} \cap \ldots \cap H_l^{'+}$ where $H_i = h * G_i$, $H_i^{'} = (h - C - mC) * G_i + C \sum a_i$. And for all $h \geq C + mC + 1$,

$$d(H_i, H_i^{'}) = \frac{|(-C - mC)\alpha_i + (C \sum a_i\,, u_i)|}{|u_i|}$$

for $i = 1, \ldots, l$, using the result above on the distance between hyperplanes. Thus, for all $i = 1, \ldots, l$, the distance $d(H_i, H_i^{'})$ remains same for all $h \geq C + mC + 1$.

Thus, fix any $h \geq C + mC + 1$. Define

$$\rho = \max\{\, \delta\big((C + mC) * \Delta\big),\; d(H_i, H_i^{'}), i = 1, \ldots, l\,\}$$

where $\delta(S)$ represents the diameter of the set S. Then ρ is independent of h. Let $z \in h * \Delta$ be an integral point with $d(z, \partial(h * \Delta)) > \rho$. Note that if $h \leq C + mC$, then by the definition of ρ, such z does not exist.

Let $F_i = H_i \cap (h * \Delta) \neq \emptyset$ be a face of $h * \Delta$ and $F_i^{'} = H_i^{'} \cap \Delta(h, C) \neq \emptyset$ be a face of $\Delta(h, C)$. Assume $z \in H_1^{'-} \setminus H_1^{'}$. Then $d(z, H_1) < d(H_1^{'}, H_1) \leq \rho$, but $d(z, F_1) > \rho$. Thus the perpendicular ray to H_1 from z does not intersect F_1 . It is a well known fact that every compact convex body in $\mathbb{R}^n$ with nonempty interior is homeomorphic to the closed n-ball, and its boundary is homeomorphic to the $(n-1)$-sphere. So $\partial(h * \Delta)$ is homeomorphic to the $(n-1)$-sphere. Thus, the perpendicular ray to H_1 from z above intersects $\partial(h * \Delta)$ somewhere, say, at z_2 which is a point of a face F_2, $F_2 \neq F_1$. Then $z_2 \in F_2 \subseteq h * \Delta$, so $z_2 \in H_1^+$. Then $d(z, F_2) \leq d(z, z_2) \leq d(z, H_1) < \rho$, a contradiction. Therefore, $z \in H_1^{'+}$. Similarly, z belongs to other $H_i^{'+}$ as well. Thus, $z \in H_1^{'+} \cap \ldots \cap H_l^{'+} = \Delta(h, C)$. Then, by Lemma 2, $z \in hA$. □

By Theorem 3, the sumset hA in $\mathbb{R}^n$ takes over the central region of dilated polytopes. Han [3] showed that, for $A \subseteq \mathbb{R}^2$ satisfying some conditions, the cardinality of hA in boundary region of dilated polytopes is a linear function of h when h is sufficiently large. For the problems counting lattice points in "thin" annuli, Wigman [8] studied the statistical behavior of the counting function. It will be interesting if we can tell something more about the density or distribution of sumsets in the boundary region.

References

[1] E. Ehrhart, *Sur un problème de géométrie diophantienne linéaire II*, J. Reine Angew. Math. **227** (1967), 25-49.

[2] S. Han, C. Kirfel and M. B. Nathanson, *Linear forms in finite sets of integers*, Ramanujan J. **2** (1998), 271-281.

[3] S. S. Han, *The boundary structure of the sumset in* $\mathbb{Z}^2$, Number theory (New York, 2003), 201-218, Springer, New York, 2004.

[4] A. G. Khovanskiĭ, *The Newton polytope, the Hilbert polynomial and sums of finite sets*(Russian), Funktsional. Anal. i Prilozhen. **26** (1992), no. 4, 57-63, 96; translation in Funct. Anal. Appl. **26** (1992), no.4, 276-281 (1993).

[5] J. Lee, *Infinitely often dense bases and geometric structure of sumsets*, Ph. D Thesis, City University of New York, 2006.

[6] M. B. Nathanson, *Sums of finite sets of integers*, Amer. Math. Monthly **79** (1972), 1010-1012.

[7] M. B. Nathanson, *Growth of sumsets in abelian semigroups*, Semigroup Forum **61** (2000), no. 1, 149-153.

[8] I. Wigman, *Statistics of lattice points in thin annuli for generic lattices*, Doc. Math. **11** (2006), 1-23 (electronic).

Department of Mathematics, Borough of Manhattan Community College, The City University of New York, 199 Chambers Street, New York, NY 10007

E-mail address: jlee@bmcc.cuny.edu